ATTACHMENT A: INVENTORY OF NCR'S APPLICATIONS

Common Name	Full Name	Function and information processed; general description of the type of information and processing provided	Platform	Number of Users
AAAP Application	Automated Advanced Acquisition Program	The automated version of AAP (AAAP) enables AAP offerors to submit and update their offers more frequently by standardizing the AAP offer submission process and by automating the AAP to support these updated procedures.	Java / Oracle 9i App Server / Oracle 9.2	750 users
CMMS	CMMS	Maximo is an Asset Management System tracking Service Calls, Inspections, Repairs, RWA service calls, Emergency Repairs, and auto-generating PM's for each building.	Java / Websphere 6 / Oracle 11g	350 full named-license users. 15 concurrent self-service license users.
Project Quest	Project Quest	The Project Quest application is a project management tool to submit, assign, track, and report on any issue with MAXIMO application.	ASP /IIS6.0/ Sql Server 2000	15 Users.
WPYG Project Tracker	Project Tracking Application (For WPYG)	logic	Java / Weblogic 8.1 App server / Oracle 10g	31 Users
TAMS	Leave Request Application	An application to track and manage leave requests.	Java / Weblogic 8.1 App server / Oracle 10g	1844 Users
Overtime Application	Overtime Application	An application to track and manage overtime request (premium pay) information.	Java / Weblogic 8.1/Oracle 10g	1800 Users
ASF Survey Application	ASF Survey Application	ASF Survey Application will allow WPF to analyze surveys from customers and supervisors concerning the performances of approximately 87 administrative support staff members. The analysis will support GSA's National Capital Region's A-76 Competitive Sourcing Program.	.NET / IIS6.0 / Sql Server 2000	71 Users
BESS	Building Emergency Support System	The application to track key information on GSA PBS NCR owned/Leased/deligated buildings to be used in emergency situations, and to make sure that their emergency preparedness is up-to-date.	.NET / IIS6.0 / Sql Server 2000	98 Users
Confined Space Program		Application to report on the number and location of confined spaces within the buildings, as well as steam tunnels and heat plants in order to obtain and track the permits given to specialists going to confined spaces for check-up and control.	.NET / IIS6.0 / Sql Server 2000	16 Users
Credit Card Tracking	Credit Card Tracking	Credit Card Tracking Application keeps track of Questionable Charges (QC) on GSA credit cards without tapping into users' personal financial info.	.NET / IIS6.0 / Sql Server 2000	39 Users

ATTACHMENT A: INVENTORY OF NCR'S APPLICATIONS

Motorpool	Motorpool	An application to maintain the NCR fleet of cars including the information on all the cars in the pool (type of vehicle, make, model, year, etc.), tracking the gas/milcage usage (beginning milcage, ending milcage), and monitoring general condition of car, etc.	.NET /IIS6.0/ Sql Server 2000	696 Users
Post Survey Tracking Application	Post Survey Tracking Application (Tenant Satisfaction Survey)	The application to assist PBS in identifying facility management patterns by tracking tenant satisfaction levels by service center and building.	.NET /IIS6.0/ Sql Server 2000	127 Users
Recycling Database	Recycling Database	The application reflects the full life cycle of recycling process in NCR.	.NET /IIS6.0/ Sql Server 2000	4 Users
Ronald Reagan Building Contracts Tracking	Ronald Reagan Building Contracts Tracking	The system is a project trackig tool for Ronal Reagan Building projects.	.NET /IIS6.0/ Sql Server 2000	10 Users (approx)
RWA Review Application	RWA Review Application	RWA 90-Day Review to assist management in reporting and analyzing, in a timely and efficient manner, the RWA's to ensure compliancy of the Acquisition Letter V-05-16.	.NET /IIS6.0/ Sql Server 2000	2474 Users
Thanks Program	Thanks Program	Application allows PBS employees to reward their collcagues in the National Capital Region for outstanding performance in support of the agency's business goals. The application serves as an on-line awards (e-commerce) store for GSA associates	.NET /IIS6.0/ Sql Server 2000	1930 Users
Triangle Contracts Tracking System	Triangle Contracts Tracking System	The application to manage contracts run by Triangle SC	.NET /IIS6.0/ Sql Server 2000	10 users (approx.)
ULO Application	Unliquidated Obligations tracking		.NET /IIS6.0/ Sql Server 2000	400 Users (approx.)
SDM Tracker	Spatial Data Management Job Tracker	Tracks jobs and manages workflow of tasks. Any user submitted requests are managed by the SDM team	.NET /IIS6.0/ Sql Server 2000	36 Users
Variance Reports	Financial Variance Reports	An application to provide the info on variances between the Planned and Actual amount of dollars for a building and/or Service Center	.NET /IIS6.0/ Sql Server 2000	10 Users (approx.)

ATTACHMENT A: INVENTORY OF NCR'S APPLICATIONS

Building Search Application	Building Search Application	A module in Insite web page. Allows searching for NCR buildings.	.NET / IIS6.0 / Sql Server 2000	Site accessible to all NCR users
~~CBT Application WBT Application~~	Web Based Asbestos Training	Provide building information about Asbestos and training related to it	.NET / IIS6.0 / Sql Server 2000	Site accessible to all NCR users
eSnap	eSnap	COTS application which provides capability to link many data sources and produce reports using the various data connections	ASP /IIS6.0/ Sql Server 2000	Site accessible to all NCR users
Exit Interview Survey	Exit Interview Survey	Application is a questionnaire that will be given to employees as part of an exit interview	ASP / IIS6.0/ Sql Server 2000	Site accessible to all NCR users
ROB Parking	ROB Parking	The ROB employees can submit their parking permit requiest via the application.	ASP /IIS6.0/ Sql Server 2000	Site accessible to all NCR users
U4P Application	Iniversity for people	The application which allows users to register for classes/training.	ASP / Sql Server 2000	Site accessible to all NCR users
Personnel /LN	Personnel Database - LotusNotes reconciliation	Enhancements to Personnel database to be reconsiled with LN. This included automating the mailing procedure, and creating an Admin console for data entry for Service Centers.	Sql Server 2000	N.A (scheduled job)
Sharepoint Sites	Events Calendar and Surveys	There are multiple sites created for both surveys and events calendar. This was done in part to migrate it from Lotus Notes.	Sharepoint 2007	All NCR users for surveys.
Conduct and Disciplinary Action Tracker	Conduct and Disciplinary Action Tracker		.NET / IIS6.0 / Sql Server 2000	TBD
Hiring Data Tracker	Hiring Data Tracker			TBD

ATTACHMENT B: INVENTORY OF NCR'S MAJOR WEBSITES

Web Site's Name	Function and information processed; general description of the type of information and processing provided	URL	Application Status	Effort
Acquisition Guidance Website	This website is designed to provide useful information and sample procurement formats to the NCR PBS acquisition community. The website is also complete with procurement links, acquisition references, and all NCR procurement bulletins.	http://insite.ncr.gsa.gov/PBS/acquisitionguidance/default.asp	Active	Weekly updates
Acquisition Community Newsletter Web site		http://insite.ncr.gsa.gov/ncr_acquisition/	Active	Minimal
APPAS	A website designed to consolidate all available materials on APPAS activities, projects, upcoming events and news..	http://insite.ncr.gsa.gov/performanceplans/	Active	Last document updates was a year ago
Business Performance Measures web page	a web page providing information regarding business performance measures	http://insite.ncr.gsa.gov/PBS/performance_measures/	Active	Weekly updates
Custodial Website	Website for Custodia Management Program providing general information about the program, custodial contract administration, commercial item specification, training availability and links.	http://insite.ncr.gsa.gov/custodial	Retired	Periodic updates
Delegations Website	The Delegations Program allows other Federal agencies to operate and maintain GSA buildings or leased space occupied by them.	http://insite.ncr.gsa.gov/delegation/	Active	No changes or Update requests Since 2 years
FDA Building Wesite	A Web site to accommodate materials pertaining to the Wiley Building -- the most significant building in the Metropolitan Service Center providing material on history and current role of the building.	http://insite.ncr.gsa.gov/fda/default.asp	Active	No changes or Update requests Since 2 years
Guild Web Site	Website consolidatin gonformation on NCR Guilds	http://insite.ncr.gsa.gov/PBS/guildsites.asp	Active	No changes or Update requests Since 4 years
Histroric Preservation	The web site provide information about the historic building preservation in NCR including list of buildings, project information and outline specifications.	http://insite.ncr.gsa.gov/historicpreservation/home.asp	Active / ??	No changes or Update requests Since 6 years
HR Web site	The HR web site is provideing information on Pay & Benefits, Retirement, Training, Work Life, Accountability, Stats, and Contacts for NCR employees.	http://insite.ncr.gsa.gov/HR/	Active	Weekely Updates

ATTACHMENT B: INVENTORY OF NCR'S MAJOR WEBSITES

HSPD-12 Information Web site (Under Development)	The HSPD-12 web site is the repository of necessary information for HSPD-12 processes and procedures.	http://insite.ncr.gsa.gov/Hspd-12/	Content transferred to Security and Emergency Management website (SEMD)	Content transferred to Security and Emergency Management website (SEMD)
IT/Computer Help Desk		http://insite.ncr.gsa.gov/ITHelpdesk/default.asp		Last document update was a yar ago
Intern Website	A website that consolidates information pertaining to NCR internship, issues such as working culture, acclimatization, guidelines for document creation and use, etc	http://insite.ncr.gsa.gov/internweb/default.asp	Active	No changes or Update requests Since 4 years
Lafayette Building Website	Website to set a goal for majority of GSA buildings to convert psychical documentation and schematics to digital web format; designed and oriented for Building Managers and project leaders to have a quick and reliable access to a large repository of information relating to the particular building.	http://insite.ncr.gsa.gov/lafayette	Active	No changes or Update requests Since 4 years
Leasing Policy & Performance Division Web site	Website dedicated to Leasing Policy and Performance Division's regional real property acquisition policies and providing guidance on leasing issues, acquisition approaches, and procedural requirements.	http://insite.ncr.gsa.gov/PBS/wpq/default.asp	Active	Monthly updates
Energy & Sustainability Website (Was split from Operation and Maintenance Web Site)	The Maintenance and Energy Web site is under development to provide general Information about the Maintenance and Energy, Services, Vertical Transfortaion, Custodial, Recycling, and Pest Management to NCR users.	http://insite.ncr.gsa.gov/maintenance_and_energy/index.shtml	Active	Frequent updates - Content and design was updated recently
Operation & Maintenance Website (Was split from Operation and Maintenance Web Site)	The Operations and Maintenance Branch's (WPMACA) mission is to provide a comprehensive facility maintenance operation to insure safe, comfortable work environments, as well as attractive and functional facilities for tenants in the National Capital Region.	http://insite.ncr.gsa.gov/operations_and_maintenance/	Active	Frequent updates - Content and design was updated recently
White Oak Bldg Complex Website	Client requested static mini portal with the information on buildings operated by the Metropolitan Service Center.	http://insite.ncr.gsa.gov/MSC	Active	weekly updates - website is being redesigned.
NCR Recycling Web Site	The NCR Recycling site is the visual front-end for the NCR Recycling Database application linked from the national GSA.gov portal.	http://ncr.gsa.gov/recycle	Active	No changes or Update requests Since 2 years
OSH Program website	A database driven Web site providing users with relevant material on OSHA (Occupational Safety and Health Act) .	http://insite.ncr.gsa.gov/PBS/OSH_Program/index.asp	Active	Weekly updates

ATTACHMENT B: INVENTORY OF NCR'S MAJOR WEBSITES

Office of Regional Counsel Website	A comprehensive website for the Office of Regional Counsel, featuring information about legal briefs, directory, and other legal links.	http://insite.ncr.gsa.gov/orc/default.asp	Active	Weekly updates
Potomac Service Center Website	Content development	http://insite.ncr.gsa.gov/potomac/	Active	Weekly updates
Procurement Management Division Web Site			Active	
Property Disposal Website	A website that provides information about Government property disposal processes and projects.	http://insite.ncr.gsa.gov/wpr	Active	Weekly updates
Regional Office Building Web site	Provide information about the General Services Administration's Regional Office Building	http://insite.ncr.gsa.gov/ROB	Development	
Rent Bill Management	one stop shopping to receive RBM updates, have questions answered, view NCR Processes and download the up-to-date versions of Rent Bill Management forms	http://insite.ncr.gsa.gov/RBM/	Active	Weekly updates
Telework Website	The Telework website assist sthe NCR Associates with NCR Flexible Workplace Program (Telework), to unify documentation, links, news, articles, –etc., helping promote the Telework concept to NCR associates and aiding them in gathering necessary information on the subject.	http://insite.ncr.gsa.gov/PBS/telework/index.asp	Active	Last updated a year ago
Triangle Website Rework	The web site provides information about Triangle Service Center	http://insite.ncr.gsa.gov/triangle	Active	Weekly updates, and montly document and links archives
U4P	The website provides Information about Services range from parking, smart cards, transit subsidy, administration of travel and purchase cards, delegations of authority, records management and other administrative services.	http://insite.ncr.gsa.gov/u4psite/	Active	Weekely Updates
Vacant Space Web site		Excel File upload under PBS Resources		
WCA Division Webpage	The website provides Information about Services range from parking, smart cards, transit subsidy, administration of travel and purchase cards, delegations of authority, records management and other administrative services.	http://insite.ncr.gsa.gov/GmaWad/WAD/wca.asp	Active	unfrequent updates

ATTACHMENT B: INVENTORY OF NCR'S MAJOR WEBSITES

RWA Committee Website	A website that provides a central repository for information on the RWA Committee meetings and current agenda, as well as a comprehensive archive of documents and relevant data.	http://insite.ncr.gsa.gov/rwa_committee/	Active	No changes or Update requests Since 3 years
Silver Spring Metro Center Web Site	Website designed and oriented for Building Managers and project leaders to have a quick and reliable access to a large repository of information relating to the particular building.	Under Development	Active	
Special Servies Division Web Site	The web site provides information about Special Services Division. The Special Services Division of NCR PBS provides the region with solutions and centers of expertise in Fire Alarms, Refrigeration & Sheetmetal, Switchgear and Move Services.	http://insite.ncr.gsa.gov/SSD/default.asp	Under Development	Under Development
Deepen & Cement Customers Relations	The objective of "Deepen and Cement Relations with Customers" is to position the NCR as a customer-focused provider of comprehensive workplace solutions.	http://insite.ncr.gsa.gov/deepen/	No updates request or changes since 2008	No updates request or changes since 2008
Internal Resources Division	Internal Resources Division provide essential management guidance, strategic planning, training and development oversight, and human resource management for PBS. The website was recently updated, but it will be moved soon under the Organizational Resources Division (ORD)	http://insite.ncr.gsa.gov/BMD/default.asp	Active	Monthly updates
Tenant Satisfaction Survey	Internal Resources Division provide essential management guidance, strategic planning, training and development oversight, and human resource management for PBS. The website was recently updated, but it will be moved soon under the Organizational Resources Division (ORD)	http://insite.ncr.gsa.gov/PBS/TSST/	Active	frequent updates -
NCR Insite	NCR INSITE	http://insite.ncr.gsa.gov/	Active	Daily Updates, changes and addtions. Plus montly document & news archiving
RA Website	NCR INSITE	http://insite.ncr.gsa.gov/AskTheRA/	Active	weekely or daily updates
Security and Emergency Management website	SEMD Provides the region with information about security, access, and emergency management programs for NCR	http://insite.ncr.gsa.gov/semd/	Active	weekly updates

ATTACHMENT C: IT SECURITY REQUIREMENTS

Contractors entering into an agreement for services to the General Services Administration (GSA) and/or its Federal customers are subject to all GSA and Federal IT Security standards, policies, and reporting requirements. The Contractor shall meet and comply with all GSA IT Security Policies and all applicable GSA and NIST standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.

Listing of References

For performance of activities for this Statement of Work, the Contractor must follow and, reference applicable security laws and regulations.

To comply with GSA Order, CIO 2100.1F, Contractors who design, operate, test, maintain, and/or monitor GSA systems must have as a minimum, the National Agencies Check with Inquiries (NACI) investigation.

The standard installation, operation, maintenance, updates, and/or patching of software should not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

Applications designed for end users should run in the standard user context without elevated system administration privileges.

The Contractor should reference and comply with the following statutes and regulations (or current versions) regarding Information Technology Security. (Please note that if a newer version of any of the following is in effect, that version supersedes the version listed below.):

GSA CIO-IT Security Procedural Guides

- GSA CIO-IT Security-01-01, IT Security Procedural Guide: Password Generation & Protection
- GSA CIO-IT Security-01-02, IT Security Procedural Guide: Handling IT Security Incidents
- GSA CIO-IT Security-01-05, IT Security Procedural Guide: Developing a Configuration Management (CM) Plan
- GSA CIO-IT Security-01-07, IT Security Procedural Guide: Access Control
- GSA CIO-IT Security-01-08, IT Security Procedural Guide: Auditing and Monitoring
- GSA CIO-IT Security-02-15, IT Security Procedural Guide: Windows 2000 Professional Hardening
- GSA CIO-IT Security-02-16/17, IT Security Procedural Guide: Windows 2000 Server Hardening Guide Package
- GSA CIO-IT Security-02-18/19, IT Security Procedural Guide: Microsoft IIS 5.0 Server Hardening Guide Package

- GSA CIO-IT Security-02-20, IT Security Procedural Guide: Sun Solaris Server Hardening
- GSA CIO-IT Security-03-22, IT Security Procedural Guide: Windows XP Professional Hardening Guide Package
- GSA CIO-IT Security-03-23, IT Security Procedural Guide: Termination and Transfer
- GSA CIO-IT Security-04-24, IT Security Procedural Guide: Home User's Guide
- GSA CIO-IT Security-04-25, IT Security Procedural Guide: Windows 2003 Server Hardening Guide Package
- GSA CIO-IT Security-04-26, IT Security Procedural Guide: FISMA Implementation
- GSA CIO-IT Security-05-27, IT Security Procedural Guide: CISCO Router Hardening
- GSA CIO-IT Security-05-29, IT Security Procedural Guide: IT Security Training and Awareness Program
- GSA CIO-IT Security-06-29, IT Security Procedural Guide: GSA Contingency Plan Testing
- GSA CIO-IT Security-06-30, IT Security Procedural Guide: Managing Enterprise Risk (Security Categorization, Risk Assessment, & Assessment & Authorization)
- GSA CIO-IT Security-06-31, IT Security Procedural Guide: Firewall Change Request
- GSA CIO-IT Security, 06-32, IT Security Procedural Guide: Media Sanitization
- GSA CIO-IT Security-06-33, IT Security Procedural Guide: McAfee VirusScan 8.5i
- GSA CIO-IT Security 07-34, IT Security Procedural Guide: CISCO CallManager and Unity Hardening
- GSA CIO-IT Security-07-35, IT Security Procedural Guide: Web Application Security
- GSA CIO-IT Security-07-36, IT Security Procedural Guide: Bluetooth Security Hardening
- GSA CIO-IT Security-07-37, IT Security Procedural Guide: Citrix Presentation Server 4 Hardening
- GSA CIO-IT Security-07-38, IT Security Procedural Guide: Hardcopy Device Security
- GSA CIO-IT Security-08-39, IT Security Procedural Guide: FY 2010 IT Security Program Management Implementation Plan
- GSA CIO-IT Security-08-40, IT Security Procedural Guide: Lotus Domino Server Security Implementation
- GSA CIO-IT Security-08-41, IT Security Procedural Guide: Web Server Log Review
- GSA CIO-IT Security-08-42, IT Security Procedural Guide: VoIP Implementation Guide
- GSA CIO-IT Security-09-43, IT Security Procedural Guide: Key Management
- GSA CIO-IT Security-09-44, IT Security Procedural Guide: Plan of Action and Milestones (POA&M)
- GSA CIO-IT Security-09-45, IT Security Procedural Guide: Oracle Database Hardening (10g, 11g)
- GSA CIO-IT Security-09-47, IT Security Procedural Guide: Hardening Virtualized Server Environments
- GSA CIO-IT Security-09-48, Security Language for IT Acquisition Efforts
- GSA CIO-IT Security-09-49, IT Security Procedural Guide: SQL Server 2008 Database Hardening

Any system/application that does not have specific GSA hardening guidance should use guidance provided by Center for Internet Security (CIS), National Security Agency (NSA), or

the Defense Information Systems Agency (DISA). If additional guidance is not provided by these sources, best practices should be followed.

GSA PBS Order

- GSA PBS 3490.1A, Document security for sensitive but unclassified building information
- GSA PBS IT Security Language for IT Acquisition Efforts Guide

GSA Orders, Policy and Standards

- GSA Order CPO 1878.1, GSA Privacy Act Program
- GSA Order CPO 1878.2, Conducting Privacy Impact Assessments (PIAs) in GSA
- GSA Order CIO P 2100.1F, GSA Information Technology (IT) Security Policy
- GSA Order CIO 2100.2A, GSA Wireless Local Area Network (LAN) Security
- GSA Order CIO 2100.3A, IT Security Training Requirement For Agency and Contractor Employees with Significant Security Responsibilities
- GSA Order CIO 2104.1, GSA Information Technology (IT) General Rules of Behavior
- GSA Order CIO 2105.1A, GSA Section 508: Managing Electronic and Information Technology for People with Disabilities
- GSA Order CIO 2106.1, GSA Social Media Policy
- GSA Order CIO 2110.2, GSA Enterprise Architecture Policy
- GSA Order CIO 2135.2B, GSA Information Technology (IT) Capital Planning and Investment Control
- GSA Order CSC 2140.1, Management of GSA's Total Web Presence
- GSA Order CIO 2140.3, System Development Life Cycle (SDLC) Policy
- GSA Order CIO 2160.2A, GSA Electronic Messaging Policy
- GSA Order CIO 2160.4, Provisioning of Information Technology (IT) Devices
- GSA Order CIO 2161.1A, Wireless Personal Digital Assistants (PDAs)
- GSA Order CIO 2180.1, Electronic Signatures to Contractually Obligate Funds
- GSA Order HCO 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- GSA Order CIO P 2181.1, Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing
- GSA Order ADM P 9732.1C, Suitability and Personnel Security

A non-disclosure agreement (NDA) is required to be signed by all Contractors who are currently not under contract with GSA in order to access the above GSA policy and procedure documentation. The Contractor should contact the Contracting Officer's Representative (COR) for the acquisition in order to obtain a copy of the NDA which must be signed and returned to the COR prior to being granted access to these documents.

Federal Laws, Regulation, and Policy

- Clinger-Cohen Act of 1996 (Public Law 104-106, Division E) (40 U.S.C. 1401(3))
- Federal Information Security Management Act (FISMA) of 2002 (H.R. 2458, Title III), E-Government Act of 2002
- Paperwork Reduction Act (PRA) of 1995 (44 U.S.C § 3506) (Public Law 104-13)
- Privacy Act of 1974 (5 U.S.C § 522a)

- Government Paperwork Elimination Act (GPEA) (Public Law 105-277)
- Government Accountability Office (GAO) GAO-09-232G
- Federal Information System Controls Audit Manual (FISCAM)
- Homeland Security Presidential Directive – 12: Policy for a Common Identification Standard for Federal Employees and Contractors

National Institute of Standards and Technology (NIST)

- Federal Desktop Core Configuration (FDCC)
- Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules
- Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
- Federal Information Processing Standard (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems, Revision 1
- Special Publication (SP) 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems
- Special Publication (SP) 800-34, Contingency Planning Guide for Information Technology Systems
- Special Publication (SP) 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems
- Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations
- Special Publication (SP) 800-53A, Guide for Assessing the Security Controls for Federal Information Systems
- Special Publication (SP) 800-57, Recommendation for Key Management – Part 2: Best Practices for Key Management Organization
- Special Publication (SP) 800-59, Guideline for Identifying an Information System as a National Security System
- Special Publication (SP) 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1
- Special Publication (SP) 800-61, Revision 1, Computer Security Incident Handling Guide
- Special Publication (SP) 800-64, Revision 2, Security Considerations in the System Development Life Cycle, Revision 1
- Special Publication (SP) 800-65, Integrating IT Security into the Capital Planning and Investment Control Process
- Special Publication (SP) 800-70, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers, Revision 1

Office of Management and Budget (OMB)

- Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Internal Control
- Office of Management and Budget (OMB) Circular A-127, Revised, Financial Management Systems
- Office of Management and Budget (OMB) Circular A-130, Revised, Transmittal Memorandum No. 4, Management of Federal Information Resources
- Office of Management and Budget (OMB) M-05-23, Memorandum for Chief Information Officers, Improving Information Technology (IT) Project Planning and Execution
- Office of Management and Budget (OMB) M-06-16, Protection of Sensitive Agency Information
- Office of Management and Budget (OMB) M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems
- Office of Management and Budget (OMB) M-04-04, E-Authentication Guidance

General Services Administration Information Technology

PBS Server Hardware and Software Technology Standards

Introduction: The purpose of this document is to outline the minimum server software and hardware requirements as documented by the PBS Regional Server Policy (rev 1.0 5/19/09).

1. Software

Product	Version
Operation System	Windows Server 2003 SP2
Oracle Database	Oracle 10g/11g
Microsoft SQL	Microsoft SQL 2005/2008
Lotus Domino	Domino 7.0.3
My SQL	My SQL 5
Microsoft Access	Microsoft Access 2003
Web Server	IIS 6.0, Apache 5.2
McAfee AntiVirus	McAfee 8.xi
Remote Control	Remote Desktop Protocol (RDP)

2. Hardware - VMWare Virtual Machine Virtual Server Standards

Item	Version
CPU	Intel Xeon E5420 @ 2.50 GHz processor
RAM	2 GB of RAM
Video	VMWare SVGA II, 16MB of Memory
Network	VMWare Accelerate AMD PCNet Gigabit Adapter

Deviations to the PBS Regional Server Minimum Standards must be approved by the Systems Integration Division manager with a waiver. The waiver can be found on ***pbsapps.gsa.gov***.

(Source: PBS Regional Server Policy 05/12/09)

Created 1/11/12

Office of the PBS
Chief Information Officer

PBS Regional Server Policy

Created by	Effective Date	Revision	Total Pages
PBS Systems Support Team	5/19/2009	1.0	32

Description

The document details the policies for the overall management of all PBS Regional Systems.

Approved by Signature

Douglas L. York **PGAC Division Director**	(b) (6)	**Date:** 05/19/09
Diane L. Herdt **PBS Chief Information Officer**	(b) (6)	**Date:** 5/19/09

Attachment E: PBS Regional Server Policy

Table of Contents

1. Key Terms

Table X Key Terms

Term	Description
PBS Regional System	Any Energy Management, Building Automation, CAD/CIFM, or PBS-related IT system server, appliance, or device that houses a regional PBS Application.
Server	Any hardware that houses a PBS Application with a Window Operating System.
Appliance	Any network attached device that is used for PBS applications (i.e. Energy metering devices/probes).
OCIO	The Office of the Chief Information Officer (OCIO) organization is temporarily responsible for backups and permanently responsible for rack space, UPS, network connectivity, and power.
Application Owner	A Government PBS Regional IT Manager, Energy Management Coordinator, or any other Government point of contact that owns an application on a PBS regional system.
Application Administrator	A technical point of contact responsible for managing an application on a PBS regional system.
ENT Shortname	An admin account for elevated rights to servers (usually first initial, middle initial & last name)
ENT Longname	A regular user account for day-to-day work. (usually first name, middle initial & last name)
Environments:	
Development	Any server or application that is used to install, configure, upgrade, change code, etc. applications.
Test	Any server or application that is used by Application Owners/Developer to test the install, configure, upgrade, change code, etc. of applications.
Staging	Any server or application that is used by PSS Team to validate the install, configure, upgrade, change code, etc. of applications.
Production	Any server or application that is used by an end-user

2. Overview

The PBS Systems Support Team (PSS Team), under the direction of the PBS Chief Information Officer (CIO) and the Systems Integration Division (PGAC), has assumed ownership of all PBS Regional Application Systems nationwide. This policy sets forth how the PSS Team will manage and support these systems.

The PSS Team will be responsible for hardware support, operating system support, database support, and ensuring the availability of the server platform hosting an application or web related software. Regional application administrators will be responsible for the administration of their specific PBS regional applications. Direct access to production and staging servers will be restricted.

	PSS Team		Regional PBS Staff	
	PROD/STAGE	TEST/DEV	PROD/STAGE	TEST/DEV
Hardware (Section 4)				
Requirements			X	X
Procurement[i]	X	X		
Installation[ii]	X	X		
Configuration[iii]	X	X		
Operating System (Section 5)				
Requirements			X	X
Installation	X	X		
Core Configuration	X	X		
Rights Management[iv]	X	X		X[v]
Key Services	X	X		X[vi]
Antivirus	X	X		
Patching	X	X		
Security	X	X		
Monitoring[vii]				
OS	X	X		X
System Hardware	X	X		X
Key Services[viii]	X	X	X	X
SQL	X	X		
Oracle	X	X		
Patching				
OS[ix]	X	X		
Win32 Application	X			X[x]
SQL DB Server	X	X		
Oracle DB Server	X	X		
Domino Server	X	X		
SQL[xi](Section 6)				
Requirements			X	X
Installation	X	X		
Configuration (Instance)	X	X		
Configuration (Indivdual Database)	X			X
Maintenance	X	X		
User Accounts	X	X		
Application Account	X			X
Permissions	X	X		

Continued

	PSS Team		Regional PBS Staff	
Oracle (Section 6)[xii]				
Requirements			X	X
Installation	X	X		
Configuration (Instance)	X	X		
Configuration (Indivdual Database)	X			X
Patching	X	X		
Maintenance	X	X		
User Accounts	X	X		
Application Account	X			X[xiii]
Permissions	X	X		
Domino (Section 6)[xiv]				
Installation	X	X		
Configuration (Instance)	X	X		
Configuration (Indivdual Database)	X			X[xv]
Patching	X	X		
Maintenance	X	X		
User Accounts	X	X		
Manager Access	X			X[xvi]
Permissions	X	X		
WIN 32 Applications (Section 8)[xvii]				
Requirements			X	X
Installation	X			X
Availability	X			X
Key Services	X			X
Admin Rights	X			X[xviii]
Service Accounts	X	X		
IIS				
Installation	X	X		
Configuration	X	X[xix]		X
Availability	X	X[xx]		
Performance	X	X		
Web Content[xxi]			X	X
Backups (Section 10)				
Agents	X	X		
Schedule	X	X		
SQL	X	X		
Oracle	X	X		
WIN 32 Application	X	X		
IIS	X	X		

	PSS Team		Regional PBS Staff	
Restore[xxii]				
Shares	X	X		
Application Data	X	X		
SQL DBs	X	X		
Oracle DBs	X	X		

[i] EMS/BAS systems will be procured by PSS team with funding coming from the regional energy budget
[ii] Installation of Hardware is being performed by PSS Team with support from GSA OCIO when required
[iii] Configuration of Hardware is being performed by PSS Team with support from GSA OCIO when required
[iv] Rights Management involves the configuring permissions on folder and files, group creation, admin/user rights on server.
[v] Regional PBS Staff can set permissions on development application servers but group creation will be done by PSS team. PSS team will also audit servers to ensure GSA IT Security compliance.
[vi] Regional Application owner can configured and document Key Services on Development Win32 Application servers since they will have admin rights to those systems. This configuration information will be used to promote the application to staging and development.
[vii] PSS Team monitors and responds to identified application specific services where information has been provided; core services will be monitored automatically and are listed on the PSS team website http://pbsapps.gsa.gov/servers/.
[viii] Regional PBS Staff can request notification when identified key application services or processes are unavailable.
[ix] OS Patching will be performed on a regular monthly schedule with development servers before production servers to test patches.
[x] Regional Application owner install and configure Win32 Application servers since they will have admin rights to those systems. This configuration information will be used to promote the application to staging and development.
[xi] The standard SQL build information will be posted on the PSS team website http://pbsapps.gsa.gov/servers/
[xii] The standard Oracle build information will be posted on the PSS team website http://pbsapps.gsa.gov/servers/
[xiii] Developers will be provided with an application DBO account in the DEV environment.
[xiv] The standard Domino build information will be posted on the PSS team website http://pbsapps.gsa.gov/servers/
[xv] Regional Application Managers will have manager rights to individual databases
[xvi] Developers will be provided with Manager Database Access in the DEV environment.
[xvii] Regional PBS Staff will have rights to install Win32 applications on development application servers. PSS team will only be able to perform restores or server rebuilds.
[xviii] Administrative rights are only given on server that are development Win32 application servers
[xix] Initial IIS Configuration will be based on PSS Team standard operations and client requirements, as provided by the client in a configuration document.
[xx] Initial IIS Configuration will be based on PSS Team standard operations and client requirements, as provided by the client in a configuration document.
[xxi] Web content access will be restricted to the home drive of the web site i.e e:\intepub\wwwroot
[xxii] PSS Team will restore files, folders, databases, or entire systems upon request.

3. PSS Standards

Administrator Access Standards

An active HSPD-12 clearance is required to access PBS or Energy Management servers.

All Application administrators will only have access any PBS Regional System which **requires** using their ENT "shortname" account (i.e. JDoe).

Standard ENT longname accounts should be used for non-administrative share access.

Hardware and Software Standards

All hardware and software requirements will be standardized and reviewed semi-annually. Deviations to the PBS Regional Server Minimum Standards must be approved by the Systems Integration Division manager with a waiver. The waiver can be found on ***pbsapps.gsa.gov***.

Table 1 Software and Hardware Standards

Product	Version
Software	
Operation System	Windows Server 2003 SP2
Oracle Database	Oracle 10g/11g
Microsoft SQL	Microsoft SQL 2005/2008
Lotus Domino	Domino 7.0.3
My SQL	My SQL 5
Microsoft Access	Microsoft Access 2003
Web Server	IIS 6.0, Apache 5.2
McAfee AntiVirus	McAfee 8.xi
Remote Control	Remote Desktop Protocol (RDP)
Hardware	
VMWare Virtual Machine	see Section 4

Networking Standards

In accordance to the GSA LAN Consolidation and Standardization (LCS) project, the PSS team will place PBS Regional servers on internal or external GSA IP addresses.

Internal GSA IP addresses will be available to the national GSA network. Inbound and outbound internet access will be restricted via proxy.gsa.gov. All stage, development, and production servers will be on the Internal GSA IP address scheme.

External GSA IP addresses will be available upon request to allow inbound and outbound internet access. All production application servers will be on the External GSA IP address scheme.

Naming Standards

The GSA Enterprise AD Naming Standards policy will be used as a guide for naming prefixes (characters 1-7) on PBS servers. The PSS team will define naming characters 8-20 on PBS servers and service accounts because the GSA Enterprise AD Naming Standards policy does not provide detailed guidance.

Table 2 Prefixes of Server Accounts and Service Accounts

Character position	Description	Resource	Symbol
1	Service	PBS	P
2-3	Region	Region number	CO, 01-11
	4-5	Site Identifier	Building Code : 01-99, AA-ZZ
6	Object Type	Service Account	B
		Server Account	S
		Global Group	G
		Domain Local	L
7	Hyphen	n/a	–

Table 3 Suffixes of Server Accounts

Character position	Description	Resource	Symbol
8-10	Function	Domino	DOM
		NetApp	NAP
		VMWare ESX Host	ESX
		PBS Energy Servers	ENG
		Application Server	APP
		SQL Server	SQL
		Oracle Server	ORA
		Web Server	WEB
11	Lifecycle Status	Production	P
		Staging	S
		Test	T
		Development	D
12-13	Ordinal Number	Ordinal Number	01, 02, 03...

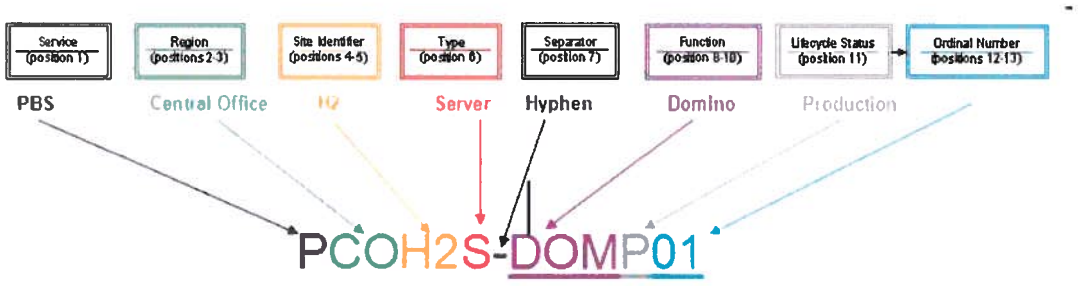


Figure X Example of naming a PBS Domino server in Production at Central Office (18th and F Streets)

Table 4 Database Instance Naming

Character position	Description	Resource	Symbol
1	Service	PBS	P
2-3	Region	Region number	CO, 01-11
4	Lifecycle Status	Production	P
		Staging	S
		Test	T
		Development	D
5-6	Application	Oracle	OR
		MS SQL	SQ
		MySQL	MQ
		Domino	DM
7-8	Ordinal Number	Instance Number	01, 02, 03...

Examples:

SQL Instances:
A database owned by PBS in Region 11 for test/lab work running SQL Server, first instance. Example: P11LSQ01

Oracle Databases:
A database owned by PBS in CO for development running Oracle, fourth instance. Example: PCODOR04

MySQL Databases:
A database owned by PBS in Region 4 for production running MySQL, third instance. Example: P04PMQ03

Table 5 Suffixes of Service Accounts

Character position	Description	Resource	Symbol
For Application Service Accounts			
8	Lifecycle Status	Production	P
		Staging	S
		Test	T
		Development	D
9-20	Application Name	N/A	Descriptive name for application
For Cluster Service Accounts			
8	N/A	N/A	Z
9-20	Cluster Root Name	N/A	name of the cluster root server name
For Windows Service Accounts			
SQL Server Named Instances			
8	Lifecycle Status	Production	P
		Staging	S
		Test	T
		Development	D
9-10	Application	Oracle	OR
		MS SQL	SQ
		MySQL	MQ
		Domino	DM
11-12	Ordinal Number	Instance Number	01, 02, 03...
13	Underscore	N/A	_
14-16	Service Type	Analysis, Reporting, or Integration	OS
		Database and Agent	SVC
SQL Server Default Instances			
8-13	Server Account Suffix	Server Name	see Table 4
14	Underscore	N/A	_
15-17	Service Type	All SQL Services	SQLSVC

Examples:
P07R7B-PBTS01
P07R7S-DBTS01

Examples:

Prod Named DB Service :
P1130B-PSQ01_SVC

Dev Default DB Service:
P07R7B-SQLD01_SQLSVC

For Windows Service Accounts (continued)

Oracle Default Instances

8-13	Last 5 characters of the Database	Database Name	see Table 4
14	Underscore	N/A	_
15-17	Service Type	All Oracle Services	SVC

MySQL Default Instances

8-13	Last 5 characters of the Database	Database Name	see Table 4
14	Underscore	N/A	_
15-17	Service Type	Database and Agent Services	SVC

Examples:

Prod Named DB Service : P05R5B-POR04_SVC

Dev Default DB Service: P07R7B-SQLD01_MQSVC

Domino Server Name (GSA Address Book):

Production
PBS-[Region]-Instance
Example: A region 3 Domino Server, second instance: PBS-03-02

Development
PBS-[Region]-DEV-Instance
Example: A region 3 Domino Server, second instance: PBS-03-DEV-01

Note:
Deviations to the PSS Naming Standards must be approved by the Systems Integration Division manager with a waiver. The waiver can be found on *pbsapps.gsa.gov*.

4. Hardware

PSS Team Responsibilities
The PSS Team is responsible for all regional PBS system hardware and storage devices. This includes provisioning new systems, storage devices, upgrades, and replacements The PSS Team will arrange physical installation or hardware replacement with OCIO when necessary.

OCIO Responsibilities
The OCIO will be temporarily responsible for backups until PBS implements a permanent backup solution. OCIO is permanently responsible for rack space, UPS, network connectivity, and power. The PSS Team will coordinate with the OCIO to resolve any network connectivity or power issues.

Table 6 Virtual Server Standards

Item	Version
CPU	Intel Xeon E5420 @ 2.50 GHz processor
RAM	2 GB of RAM
Video	VMWare SVGA II, 16MB of Memory
Network	VMWare Accelerate AMD PCNet Gigabit Adapter

Deviations to the Virtual Server Standards must be approved by the Systems Integration Division manager with a waiver. Non-standard requests may call for procurement. The waiver can be found on *pbsapps.gsa.gov*.

Hardware Issues:
In the event of a hardware failure or replacement, the PSS Team may dispatch its own team member, an OCIO technician, or regional PBS technician to resolve the issue. Access to the server room at Regional Office Buildings will be coordinated with the Regional PBS POC or the OCIO POC.

5. Operating System (OS) Standards

The PSS Team is solely responsible for installing, configuring, patching, securing, and maintaining all system files of the Operating System.

All new PBS systems must:

- Be on the GSA Network
- Be on the ENT Domain
- Reside under the PBS OU Structure in Active Directory
- Point their Primary and Secondary DNS to the GSA ENT DNS Servers
- Adhere to the PBS Naming Standards (See Section 2)
- Separate OS files/application data/temp files in the following manner:
    - System Drive (C:\) – operating system files (backed up to regional NetApp)
    - Memory Swap File (D:\) – pagefile.sys (not backed up)
    - Application Data (E:\ and/or others depending on system requirement) applications installed and data (backed up to national NetApp)
    - Temp Data (F:\) – any temp or install files (not backed up)

6. Database Access

The PSS Team is responsible for installing, configuring, patching, securing, and maintaining all aspects of any Microsoft SQL, MySQL, Oracle, and Domino servers. Any deviations from the following standards will require a waiver.

Microsoft SQL Configuration and Access Standards

SQL Server 2005 Standard Edition is the current standard. All configurations related to the Installation of any SQL Server Components such as Reporting, Integration and Reporting services will be handled by the PBS Systems Support Team.

Table 7 Microsoft SQL Database Configuration

Configurations	Production	Staging/Test	Development
SQL 2005/2008 Standard Edition	✓	✓	✓
Installation on Data Drive (E:\)	✓	✓	✓
Database service using ENT Service Account	✓	✓	✓
Mixed mode authentication	✓	✓	✓
Named Instance on Production Server	✓	✓	✓
Full Backup Model	✓	✗	✓
Simple Backup Model	✗	✓	✗

Production Access Rights:

- Application Account - The application will have an account created for connection to the database. This will be via an SQL account that is given 'db_owner' role to perform all activities in the database.
- Application Administrators/Developers – No access to the database.

Staging Access Rights:

- Application Account - Same as Production
- Application Administrators/Developers – Same as Production

Test Access Rights:

- Application Account - Same as Production
- Application Administrators/Developers – Same as Development

Development Access Rights:

- Application Account - Same as Production
- Application Administrators/Developers – A Windows user group will be created. The ENT admin "shortname" domain account of Application administrators/developers will be assigned to this Windows group for accessing database. This group will be assigned with the following privileges via a role for corresponding application database(s):
    - db_owner
    - Alter Trace
    - DBCREATOR

Deviations to the Microsoft SQL Configuration and Access Standards must be approved by the Systems Integration Division manager with a waiver. The waiver can be found on *pbsapps.gsa.gov*.

MySQL Configuration and Access Standards

MySQL configuration will use a full backup model in Production, Staging, and Development environments.

Production Access Rights:

- Application Account - The application will have an account created for connection to the database. This will be via a MySQL account that is given "Schemata Owner" role to perform all activities in the database.
- Application Administrators/Developers – No access to the database.

Staging Access Rights:

- Same as Production

Test Access Rights:

- Same as Development

Development Access Rights:

- Application Account (same as Production Environment) – The application will have an account created for connection to the database. This will be via a MySQL account that is given "Schemata Owner" role to perform all activities in the database.
- Application Administrators/Developers – A MySQL user will be created. This user will be assigned with "Schemata Owner" or Root database role for corresponding application database. The short name Windows account of Application administrators/developers will be assigned to this Windows group for accessing database.

Deviations to the MySQL Configuration and Access Standards must be approved by the Systems Integration Division Manager with a waiver. The waiver can be found on *pbsapps.gsa.gov*.

Oracle Configuration and Access Standards

Table 8 Oracle Database Configuration

Configurations	Production	Staging/Test	Development
Oracle 10g/11g	✓	✓	✓
Installation on Data Drive (E:\)	✓	✓	✓
Home: E:\oracle\product\version(10.2.0) or (11.1.0)\db_1	✓	✓	✓
Database service using ENT Service Account	✓	✓	✓
Archive Log Mode	✓	×	×

Production Access Rights:

- Application Account - The application account/schema will have all the necessary privileges that it needs to function as requested by the application owner. Sysdba, system, and/or sys access will not be granted.
- Application Administrators/Developers – No access will be granted to developers on the production instance(s). Read privileges(select) to the tables may be granted but will require a waiver. Access will be via a role which can be granted to the appropriate user ID.

Staging Access Rights:

- Same as Production

Test Access Rights:

- Same as Development

Development Access Rights:

- Application Account – Same as Production
- Application Administrators/Developers – Roles will be created at the schema level for the instance to allow the developer to perform the following types of actions:
  - create/modify/drop tables
  - create/modify/drop views
  - create/modify/drop grants
  - create/modify/drop sequences
  - create/modify/drop procedures
  - Create User
  - IMP_FULL_DATABASE
  - CREATE DATABASE LINK
  - CREATE DIMENSION
  - CREATE INDEX
  - CREATE MATERIALIZED VIEW
  - CREATE SYNONYM
  - CREATE TABLESPACE
  - CREATE TRIGGER
  - CREATE TYPE
  - QUERY REWRITE
  - SELECT ANY DICTIONARY

Deviations to the Oracle Configuration and Access Standards must be approved by the Systems Integration Division Manager with a waiver. The waiver can be found on *pbsapps.gsa.gov*.

Domino Configuration and Access Standards

Domino configuration will use a full backup model in Production, Staging, and Development environments.

Table 9 Domino Access

Role Name	Developer Account
Production and Staging Environments	
Editor Access	✓
Manager Access	×
Development Environment	
Editor Access	✓
Manager Access	✓

Deviations to the Domino Configuration and Access Standards must be approved by the Systems Integration Division manager with a waiver. The waiver can be found on *pbsapps.gsa.gov*.

7. Energy Management

All Energy Management Windows-based servers, including Energy Metering servers and Building Automation servers, will be managed by the PSS Team in accordance with this document.

All Energy Management servers must:

- Be on the GSA Network
- Be on the ENT Domain
- Adhere to the PBS Naming Standards (See Section 2)

PSS Responsibilities

- Setup hardware at Central Office or remotely using the Dell Remote Access Card
- Dell Remote Access cards will be used to access remote EM servers
- Monitor operating systems, databases, and applications for availability and health
- Updates to the operating system, database, and anti-virus software
- Perform security scans on servers using McAfee FoundStone
- Address security vulnerabilities
- Appliances will not be supported
- Provide temporary administrative rights only as necessary

Procurement

The regional Energy Management office will be financially responsible for all Energy Management servers and associated software that is located outside of the Regional Office building. PBS Central Office will be responsible for processing the procurement using funds from the regional Energy Management office.

A standard Energy Management Server configuration can found on http://pbsapps.gsa.gov/servers/energy_specs.html.

Deviations to the PBS Energy Management Standards must be approved by the regional EMS POC and Systems Integration Division manager with a waiver. The waiver can be found on *pbsapps.gsa.gov*.

Any deviation from these policies will require a signed waiver by the regional EMS POC and the PBS CIO Systems Integration Division Director. An online waiver form can be found at http://pbsapps.gsa.gov.

8. Applications

The PSS Team will monitor the functionality of Win32 or IIS PBS registered applications in the production environment upon request by the Application Owner.

Win32 Applications

Server Configuration
All Win32 Applications must be installed on the Data drive (E :\) to separate the operating system from the application, optimize the backup replication, and restore processes. Win32 Applications installed in the staging and production environments are exceptions to the application waiver. Configuration and creation of service accounts will be done by the PSS team.

Server Rights and Responsibilities
Production/Staging Environment
Application Administrators/Developers will not have rights to production or staging application servers. The PSS Team will monitor production and staging servers.

Development/Test Environment
Application Administrators/Developers will be granted full administrator rights to the development application server to install, change, configure settings. The PSS Team will not monitor development servers. However, OS maintenance will be done on Win32 systems by the PSS team.

New PBS Applications
All new and existing PBS applications should be registered in the Application Registration System (ARS). ARS information can be found on the PBS Portal (http://pbsportal.pbs.gsa.gov).

IIS Applications

Server Configuration
IIS will be hosted on web servers in all environments. The web servers will host multiple sites.

Remote Access
Remote Windows access will not be permitted to the IIS server. IIS sites can be accessed and modified by share access to the site's individual home directory—not the webroot$ directory.

Server Rights and Responsibilities
Production/Staging Environment
Modify Access will be granted to the website home directory via a mapped drive.

Development/Test Environment
Modify Access will be granted to the IIS Home Directory via a mapped drive.

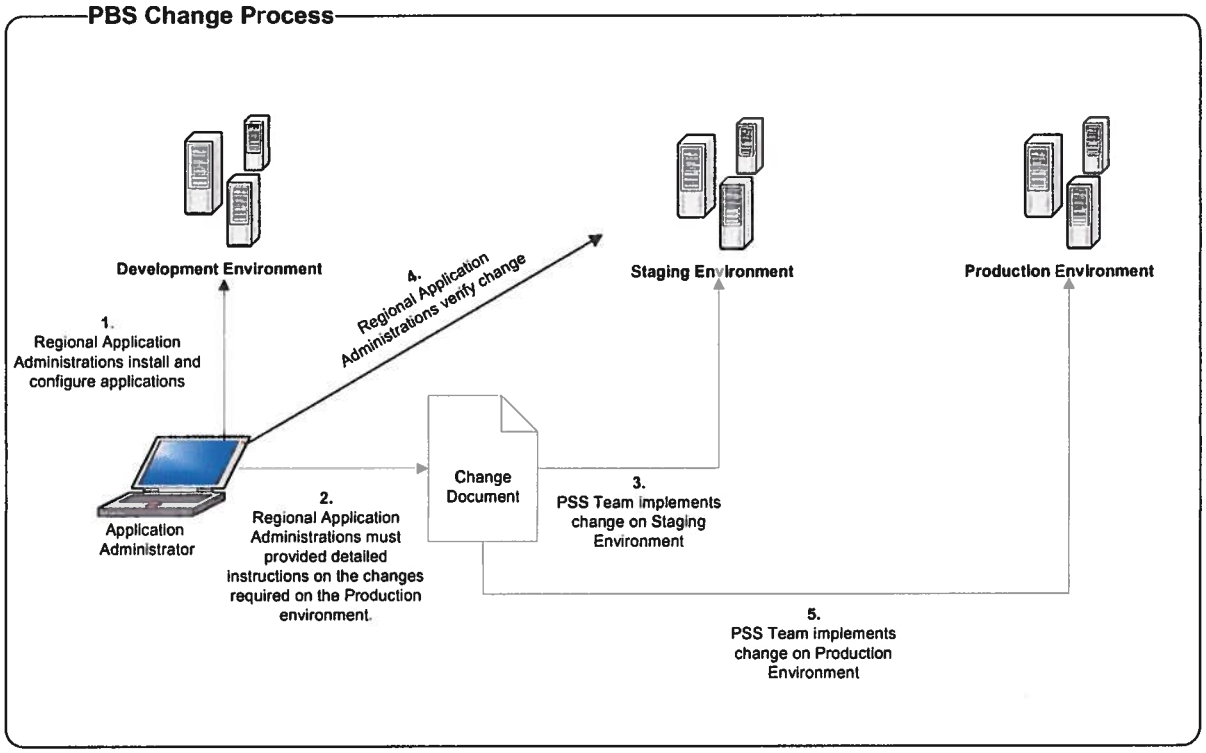
Restart IIS permissions
The IIS server will only be restarted by the PSS team upon approval by all application administrators and Government POCs with sites on the IIS Server

Other Web Server Applications
Access to other Web applications such as Weblogic/Websphere/Apache/Tomcat will be addressed on a case by case basis.

9. Change Management

Any changes to the hardware, operating system, database application, application software, etc., must be processed through the Change Control process established by the PSS Team. All changes will require a government regional POC approval.

The chart below describes a typical change process:



The SLA for a change is dependent of the scope of the change.

10. Backup & Restore

The Office of the Chief Information Officer will continue to provide backup services to all PBS Applications systems nationwide using their existing backup software and hardware. The PSS team will assume all backup services from the OCIO once the planned NetApp backup solution is implemented. Once implemented, this section will have our backup retention policies for data and time of storage.

Once the NetApp solution is in place, the following guidelines will be followed:

Backup Retention

Windows System

- Production
  - Production system drives (C:\) will be backed up daily on the local NetApp system but not replicated or archived to tape.
  - Production data drives (E:\) will be backed up daily on the local NetApp systems in each region and will be retained for up to 60 days (30 minimum). This will allow the PSS team provide daily restore granularity (Monday - Friday).
  - Production data drive backups will be replicated daily (Monday – Friday) to an off-site NetApp system and then archived to tape at the Enterprise Service Center (ESC) and the restore granularity will be monthly. *See Appendix A – Backup Diagram.*
  - All Production data drives will be replicated to the ESC and archived to tape with a retention period of thirteen (13) months.
- Staging/Test
  - No Backups will be performed.
  - Stage servers will be backed up via VMWare snapshot utility based on updates/changes to the stage servers.
- Development
  - Data on Development servers on both system (C:\) and data drive (E:\) will be kept for up to 30 days on the NetApp system each region.
  - Development data will not be replicated or archived to tape.
  - If longer development retention is needed, a request can be made to the PSS team to establish an agreeable solution and timeframe.

Oracle

- Production
  - All databases will be in 'ARCHIVELOG' mode (can be recovered to a specific point in time)
  - Daily Full Exports
    - A daily full export of the database will be taken. The .dmp file and log file will go to the local NetApp Share in a directory structure similar to this: \\RegionalNetappServer\dbbackups\Oracle\DatabaseServerName\InstanceName
    - Three (3) days worth of export will be available at all times on the local NetApp Share. The oldest export in the directory will be deleted automatically after 3 days.
  - Daily Hot Incremental Backups
    - Hot incremental backups will be performed using SyncSort. The SyncSort backup will consist of the controlfile, datafiles, and archivelogs. The backups are OS backup copies of the datafiles, controlfiles, and archivelog generated during the backup. These files are cataloged with RMAN so that they can be used for restore and recovery operations using RMAN.
  - Weekly Cold Backup using RMAN
    - A cold backup of the database will be taken on a weekly basis. The backup will go to the local NetApp Share in a directory structure similar to this: \\RegionalNetappServer\dbbackups\Oracle\DatabaseServerName\InstanceName\WEEKLY_COLD_BACKUPS . The RMAN retention policy will be set to 2.
- Staging/Test
  - All databases will be in 'NOARCHIVELOG' mode
  - No Backups will be performed.
- Development
  - All databases will be in 'NOARCHIVELOG' mode
  - Daily Full Exports – Same as Production
  - Daily Hot Incremental Backups - None
  - Weekly Cold Backup using RMAN – Same as Production

MS SQL

- Production
  - All databases will be in 'full recovery model' unless not required
  - All databases will have replicated backups up via SyncSort.
  - All databases will have local backups implemented with one MS SQL Maintenance Plan. This will include
    - Full daily backups
    - Database Validation
    - Transaction Log Backups every 5 hours from 5AM to 8PM, Monday – Friday
    - Updating Stats
    - Database Shrinking for growth above 100MB
    - The naming convention will be as follows: DB MP ServerName-InstanceName i.e. DB MP PCOH2S-SQLP01-PCOSQP01

- Staging/Test/Development
  - All databases will be in 'full recovery model' unless not required
  - All databases will have local backups implemented with one MS SQL Maintenance Plan. This will include
    - Full daily backups
    - Database Validation
    - Transaction Log Backups every 5 hours from 5AM to 8PM, Monday – Friday
    - Updating Stats
    - Database Shrinking for growth above 100MB
    - The naming convention will be as follows: DB MP ServerName-InstanceName i.e. DB MP PCOH2S-SQLD01-PCOSQD01

Restore Policy

High Severity
An application, database or server hardware has crashed or critical data files have been deleted or corrupted. A full application, database or server hardware recovery is required to restore functionality to the application.

Time to restore/repair:

High Severity Full System Crash: Up to 24-36 hours from time of new hardware acquisition if full server failure and data is being restored from within 30 days on local backup. The restore could be longer if restoring from older than 30 days depending on amount of data that might need to be replicated back to source site. (WAN speeds will play into that timeframe).

High Severity File/Data Restore: Initial file/data restore to be initiated within 2 hours (If data is within 30 days; if older it can take longer since data will have to come from replicated mirror.) of restore request for a file/data level or DB restore during normal business hours (after hours on a case by case basis). Actual restore time of data if within 30 days should be under 2 hours depending on size of restore. If older than 30 days times can vary widely based on WAN speeds and size of data.

Normal Severity
The server, application, or database remains operational but some files/data may not function correctly or software has been accidentally deleted and requires restoration.

Time to restore/repair:
For file/data restores classified as normal priority up to 8 hours.

Low Severity
Restores of this level may be requested to test for integrity of backups or non-critical restores.

Time to restore/repair:
Response time for backups with a Low priority is three (3) working days.

11. COOP

Current Initiatives
The PSS Team will work with each region to identify their COOP application and classify them into one of the following tiers:

- Tier 1 – Availability required within 24 hours
- Tier 2 – Availability required within 24-48 hours
- Tier 3 – Availability not required for COOP

6 month – 1 year Plan
The PSS Team will refresh all COOP servers with newer hardware using VMware. All Tier 1 Applications will be migrated including developing a comprehensive disaster recovery plan for each Tier 1 application.

Future Solution
The PSS Team will work to develop a comprehensive disaster recovery plan for all applications in a regional site using a combination of VMWare and NetApp technologies.

12. Maintenance

The PBS Systems Support Team will have the following daily maintenance window for production systems:

Sunday – Saturday 8PM – 10PM (ET)

The PBS Systems Support Team will have the following daily maintenance window for staging/test/development systems:

Monday - Friday 7AM – 6PM (ET)

Maintenance will be performed during these times on an as needed basis. The affected region(s) will be notified prior to any maintenance taking place to provide time for Regional Application owners to notify their customers.

Monthly patching will be performed on the third weekend of the month.

Saturday 6AM – Sunday 10PM (ET)

Please refer to http://pbsapps.gsa.gov for a complete patching schedule.

13. Purchasing

Hardware:
All server-based hardware purchases and database software will be processed through the PBS Systems Integration Division Director, with the exception of Energy Management and Building Automation servers (*refer to the Energy Management section*). This includes any server-class system, any network attached appliance, and any storage device.

Software:
All Operating Systems Software will be purchased and managed by the PSS team with approval from the PBS Systems Integration Division Director.

Database Software (MS SQL / Oracle / Domino) versions will be purchased by the PSS Team as long as it is for an upgrade and/or consolidation of database servers. A one-to-one or many-to-one migration will be covered under this guidance. Any new database server or additional options will be purchased by the Regional Application Owners.

Win32 Applications will be purchased by the Regional Application Owners with a copy of the software provided to the PSS team for Configuration Management and production installation with documentation (see section 8 & 9).

14. Support

The PBS Systems Support Team is available 24 hours a day, 7 days a week. Normal business hours are Monday – Friday, 7:00am – 7:00pm ET. Outside normal business hours, we have staff that is available on an on-call basis for productions systems. Support for Stage and Development environments will be restricted to normal business hours unless agreed upon by Application Owner and the Systems Integration Division.

Contact Information

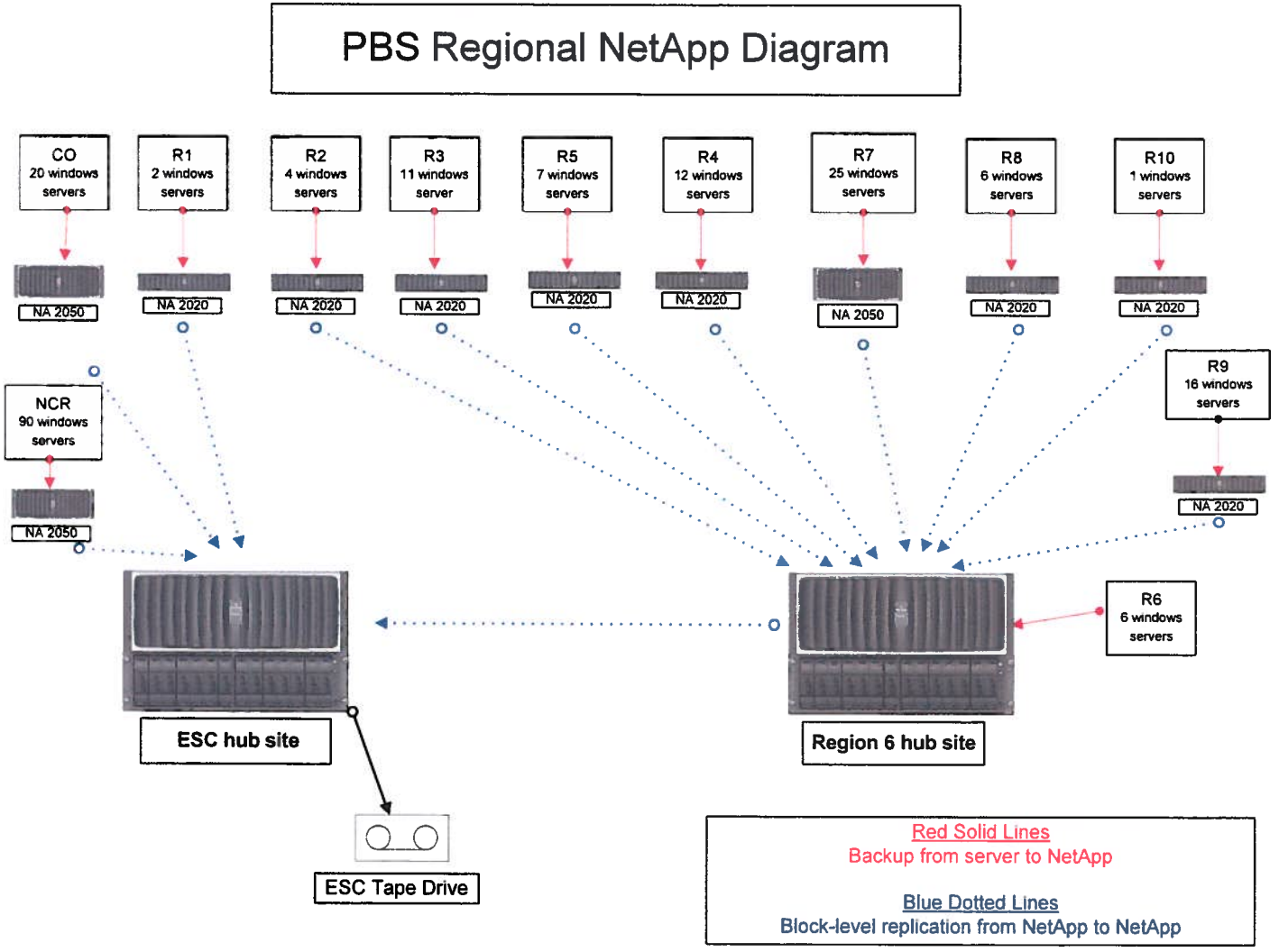
Email: pbssystem.support@gsa.gov
Phone: (866) 274-0781
Website: http://pbsapps.gsa.gov

15. Review History

Enter complete information for the change request in the table below.

Date	Reviewer Name	Reviewer Role	Change/Information Affected
8/08/08	Allen Samuel	Creator	Initial Creation.
11/21/08	Michael Warch	Editor	Edit Formatting.
11/24/08	Allen Samuel	Editor	Various Changes
12/1/08	Doug York	Reviewer	
12/2/08	Allen Samuel	Editor	
2/25/09	Allen	Editor	Added Chart and Diagram
4/15/09	Jason Boig	Editor	Updated Draft 2 and revised all formatting
5/8/09	Jason Boig	Editor	Updated changes to Draft 3
5/15/09	Jason Boig	Editor	Updated to Version 1.0 and submit for approval / signatures

Appendix A Backup Diagram



Attachment F: Cost Estimate Sheet

BASE PERIOD

CLIN	DESCRIPTION	PRICING TYPE	Quantity	Unit Price	Total Firm Fixed Price
0001	Operations and Maintenance (O&M)	FFP			
0002	Travel and ODC	NTE $50,000			
	Sub -Total				

OPTION PERIOD: 1

CLIN	DESCRIPTION	PRICING TYPE	Quantity	Unit Price	Total Firm Fixed Price
0003	Operations and Maintenance (O&M)	FFP			
0004	Help Desk Support	FFP			
0005	Travel and ODC	NTE $50,000			
	Sub -Total				

OPTION PERIOD: 2

CLIN	DESCRIPTION	PRICING TYPE	Quantity	Unit Price	Total Firm Fixed Price
0006	Operations and Maintenance (O&M)	FFP			
0007	Help Desk Support	FFP			
0008	Travel and ODC	NTE $50,000			
	Sub -Total				

OPTION PERIOD: 3

CLIN	DESCRIPTION	PRICING TYPE	Quantity	Unit Price	Total Firm Fixed Price
0009	Operations and Maintenance (O&M)	FFP			
0010	Help Desk Support	FFP			
0011	Travel and ODC	NTE $50,000			
	Sub -Total				

OPTION PERIOD: 4

CLIN	DESCRIPTION	PRICING TYPE	Quantity	Unit Price	Total Firm Fixed Price
0012	Operations and Maintenance (O&M)	FFP			
0013	Help Desk Support	FFP			
0014	Travel and ODC	NTE $50,000			
	Sub -Total				

	Total Firm Fixed Price Proposed Base + Options

 # THE NTE CEILING AMOUNT REPRESENTS THE MAXIMUM AMOUNT OF THE GOVERNMENT'S LIABILITY. THE CONTRACTOR EXCEEDS THE CEILING AT ITS OWN RISK.

 # Contract Access Fee (CAF) Remittance will be paid in accordance with Alliant Small Business GWAC Ordering Guide instruction addressed in Section G.9.5

Attachment G: Past Performance Questionnaire

INFORMATION TECHNOLOGY SYSTEM SUPPORT
Requirement
National Capitol Region, Washington, DC

PAST PERFORMANCE QUESTIONNAIRE

Your assistance is requested in support of a source selection.

Please complete this Questionnaire no later than 1/27/2012 and mail, scan to email or send by facsimile to:

Carlos C. Carter Sr.
Contract Specialist
Acquisition Management Division (WP3PQ)
Public Building Services
National Capital Region
U.S General Services Administration
301 7th &D Streets, SW #7719
Washington DC. 20407-0001
(202) 997-4526 Cell
(202)708-9497 Office
(202)401 6075 FAX
carlos.carter@gsa.gov

When complete, the information on this form is SOURCE SELECTION SENSITIVE INFORMATION (41 U.S.C. 423) and shall be protected accordingly.

TO BE COMPLETED BY OFFEROR

1. CONTRACTOR NAME & ADDRESS:	2. CONTRACT NO.:
	3. CONTRACT INITIATION DATE:
	4. COMPLETION DATE: Present
	5. CONTRACT VALUE (with options):
	6. TYPE OF CONTRACT:

7. DESCRIPTION OF CONTRACT REQUIREMENTS: Six people ranging from Administration to various accounting functions.

Please add a continuation page if additional space necessary.

TO BE COMPLETED BY PAST PERFORMANCE REFERENCE AT EVALUATING ORGANIZATION

8. EVALUATION: a. NAME, POSITION (Project Manager/ COR/ Other) AND ORGANIZATION:

b. PHONE NUMBER: c. FAX NUMBER:
d. MONTHS OF PERFORMANCE MONITORED: e. DATE: f. SIGNATURE:

Please circle the response code for each topic (A – G) that best reflects your experience with this contractor.

O = Outstanding **A** = Adequate **P** = Poor
E = Excellent **M** = Marginal **N/O** = Not Observed

A. **Quality of Products and Services** - Assess the contractor's conformance to contract requirements, specifications, and standards of good workmanship (e.g., technical, professional, environmental, or safety and health standards). Evaluate the effectiveness of the contractor's overall quality control procedures and safety program or efforts.

B. **Performance** – Assess the contractor's performance as the General Contractor or Architect/Engineer (as appropriate) for the project. Evaluate the contractor's overall technical competence.

O E A M P N/O

C. **Schedule** – Assess the timeliness of contractor against the schedule of activities. Evaluate the contractor's responsiveness to contract, program an/or schedule changes.

O E A M P N/O

D. **Technical Requirements** – Assess the contractor's ability to fulfill the technical requirements of the contract. Assess the contractor's ability to overcome technical problems, labor issues, and/or other performance difficulties

O E A M P N/O

E. **Cost Control** – Assess the contractor's ability to manage the contract budget and control costs.

O E A M P N/O

F. **Customer Satisfaction** – Assess the contractor's responsiveness to customer concerns and "user friendliness". Evaluate the contractor's overall commitment to quality performance and customer satisfaction. Evaluate the contractor's cooperation and willingness to work as a team (with your personnel, other contractors, etc.)

O E A M P N/O

G. **Personnel** - Assess the availability, adequacy, and suitability of the contractor's staffing for the work required. Assess the quality and stability of the contractor's workforce.

O E A M P M/O

H. MANAGEMENT - Assess the effectiveness of the contractor's on-site management and supervision including the contractor's ability to plan and conduct operations in the most cost effective manner.

O E A M P M/O

I. **Overall Assessment.**

O E A M P N/O

If an Award Fee contract, what was the average Award Fee % earned?

ORGANIZATIONAL CONFLICT OF INTEREST

I. INSTRUCTIONS

Read Part II carefully. If a disclosure statement is required, complete Part III. If a representation is submitted, complete Part IV. Complete Part V in every case.

II. ORGANIZATIONAL CONFLICT OF INTEREST DISCLOSURE OR REPRESENTATION

It is General Services Administration (GSA) policy to avoid situations which place an offeror in a position where its judgment may be biased because of any past, present, or currently planned interest, financial or otherwise, the offerer may have which relates to the work performed pursuant to this solicitation or where the offeror's performance of such work may provide it with an unfair competitive advantage. (As used herein "offeror" means the proposer or any of its affiliates or proposed consultants or subcontractors of any tier.)

Therefore:

(a) The offeror shall provide a statement which describes in a concise manner all relevant facts concerning any past, present or currently planned interest (financial, contractual, organizational, or otherwise) relating to the work to be performed hereunder and bearing on whether the offeror has a possible organizational conflict of interest with respect to (1) being able to render impartial, technically sound, and other objective assistance or advise, or (2) being given an unfair competitive advantage. The offeror may also provide relevant facts that show how possible organizational conflict of interest relating to other divisions or sections of the organizations and how that structure or system would avoid or mitigate such organizational conflict.

(b) In the absence of any relevant interest referred to above, the offeror shall submit a statement certifying that to its best knowledge and belief no such facts exist relevant to possible organizational conflicts of interest. Proposed consultants and subcontractors are responsible for submitting information and may submit it directly to the Authorized Representatives of this solicitation.

(c) Authorized Representative will review the statement submitted and may require additional relevant information from the offeror. All such information, and any other relevant information will be used by GSA to determine whether an award to the offeror may create an organizational conflict of interest. If found to exist, GSA may direct Authorized Representative to (1) impose appropriate conditions which avoid such conflict, (2) disqualify the offeror, or GSA may determine that it is otherwise in the best interest of the United States for Authorized Representative to contract with the offeror by including appropriate conditions mitigating such conflict in the contract awarded.

(d) The refusal to provide the disclosure or representation of any additional information as required shall result in disqualification of the offeror for award. The nondisclosure or misrepresentation of any relevant interest may also result in the disqualification of the offeror for award, or if such nondisclosure or misrepresentation is discovered after award, Authorized Representative may terminate the contract for default, recommend that GSA disqualify the contractor from subsequent related contracts, or be subject to such other remedial actions as may be permitted or provided by law. The attention of the offeror in complying with this provision is directed to

18 U.S.C. 1001 and 31 U.S.C. 3802(a)(2).

(e) Depending on the nature of the contract activities, the offeror may, because of possible organizational conflicts of interest, propose to exclude specific kinds of work from the statement, unless the solicitation specifically prohibits such exclusion. Any such proposed exclusion by an offeror shall be considered by Authorized Representative in the evaluation of proposals, and if Authorized Representative considers the proposed excluded work to be an essential or integral part of the required work, the proposal may be rejected as unacceptable.

(f) No award shall be made until the disclosure or representation has been evaluated by GSA. Failure to provide the disclosure or representation will be deemed to be a minor informality and the offeror or contractor shall be required to promptly correct the omission.

III. DISCLOSURE STATEMENT: (attach additional pages if more space is needed)

IV. REPRESENTATION

The offeror, _____, hereby represents that it is aware of no past, present, or currently planned interest (financial, contractual, organizational, or otherwise) relating to the work to be performed under the contract resulting from Request for Proposal No. _____ that would indicate any impingement upon its ability to render impartial, technically sound, and objective assistance or advice or result in it being given an unfair competitive advantage. This representation applies to all affiliates of the offeror and its proposed consultants or subcontractors of any tier.

V. SIGNATURE

Offeror's Name_____

RFP/Contract No._____

Signature_____

Title_____

Date_____

Security Clause - HSPD 12 Standard Language

52.204-9 Personal Identity Verification of Contractor Personnel.

As prescribed in 4.1303, insert the following clause:

PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (SEPT 2007)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

(End of clause)

552.237-70 Qualifications of Offerors.

As prescribed in 537.110(a), insert the following provision:

QUALIFICATIONS OF OFFERORS (JUNE 2009)

(a) Offers will be considered only from responsible organizations or individuals now or recently engaged in the performance of building service contracts comparable to those described in this solicitation. To determine an Offeror's qualifications, the Offeror may be requested to furnish a narrative statement listing comparable contracts which it has performed; a general history of its operating organization; and its complete experience. An Offeror may also be required to furnish a statement of its financial resources; show that it has the ability to maintain a staff of regular employees adequate to ensure continuous performance of the work; and, demonstrate that its equipment and/or plant capacity for the work contemplated is sufficient, adequate, and suitable.

(b) Competency in performing comparable building service contracts, demonstration of acceptable financial resources, personnel staffing, plant, equipment, and supply sources will be considered in determining whether an Offeror is responsible.

(c) Prospective Offerors are advised that in evaluating these areas involving any small business concern(s), any negative determinations are subject to the Certificate of Competency procedures set forth in the Federal Acquisition Regulation.

(End of provision)

552.237-71 Qualifications of Employees.

As prescribed in 537.110(a), insert the following clause:

QUALIFICATIONS OF EMPLOYEES (MAY 1989)

(a) The contracting officer or a designated representative may require the Contractor to remove any employee(s) from GSA controlled buildings or other real property should it be determined that the individual(s) is either unsuitable for security reasons or otherwise unfit to work on GSA controlled property.

(b) The Contractor shall fill out and cause each of its employees performing work on the contract work to fill out, for submission to the Government, such forms as may be necessary for security or other reasons. Upon request of the Contracting Officer, the Contractor and its employees shall be fingerprinted.

(c) Each employee of the Contractor shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by Alien

Registration Receipt Card Form I-151, or, who presents other evidence from the Immigration and Naturalization Service that employment will not affect his immigration status.

(End of clause)

H-X. COMPLIANCE WITH SECURITY REQUIREMENTS

(a) The Contractor shall comply with all GSA and tenant agency security requirements in the building(s) where work is being performed.

(b) When a controlled personnel identification access system is used by a tenant agency at a site where work is performed, the tenant agency will be responsible for providing any required access credentials. Credentials shall be displayed at all times or as otherwise required by the tenant agency.

H-X. IDENTIFICATION CREDENTIAL

(a) Upon receipt of a favorable suitability determination, each Regular or Temporary Employee shall be issued an identification credential (Credential) permitting regular access to the building(s) were work is being performed.

(b) Regular or Temporary Employees with Credentials shall be required to comply with all applicable access security screening procedures applicable to Government or other personnel possessing similar Credentials.

(c) All Contractor or subcontractor employees possessing Credentials shall visibly display their Credentials at all times while in the building(s) where work is being performed.

(d) The Contractor shall be responsible for ensuring that all identification credentials are returned to the Government when a particular Contractor or subcontractor employee will no longer be providing service under the Contract at the building(s) covered by the Credential.

(e) The Contractor will notify the Government when Credentials are lost. In that event, the Contractor will be responsible for reimbursing the Government for its cost in issuing a replacement Credential.

H-X. STANDARDS OF CONDUCT

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance, and integrity and shall be responsible for taking such disciplinary action with respect to its employees as may be necessary.

H-X. REMOVAL FROM CONTRACT WORK

(a) As provided in the clause entitled "Qualifications of Employees", the contracting officer or a designated representative may require the Contractor to remove any employee(s) from GSA controlled buildings or other real property should it be determined that the individual(s) is either unsuitable for security reasons or otherwise unfit to work on GSA controlled property. This shall include, but not be limited to, instances where an employee is determined, in the Government's sole discretion, to be incompetent, careless, insubordinate, unsuitable or otherwise objectionable.

(b) A contractor employee may also be removed where the continued employment of the contractor employee in connection with the Government work is deemed, in the Government's sole discretion, contrary to the public interest, inconsistent with the best interests of security, or a potential threat to the health, safety, security, general well being or operational mission of the facility and its population.

(c) Where a contractor employee is granted a temporary suitability determination, and an unfavorable final suitability determination is later rendered, the Government may insist on the employee's removal from the work site and from other work in connection with the Contract.

(d) The Contractor shall be responsible for providing replacement employees in cases where contract employees are removed at no additional cost to the Government.

H-X. SENSITIVE BUT UNCLASSIFIED (SBU) BUILDING INFORMATION

Dissemination of sensitive but unclassified paper and electronic building information shall be made on a "need to know" basis in accordance with GSA Order PBS P 3490.1A, a copy of which will be made available upon request.